Security Information & Resources on the Internet

Wendall Mayson, wendall.mayson@srs.gov
F. Arthur Cochrane, arthur.cochrane@srs.gov

Westinghouse Savannah River Company

Savannah River Site

Aiken, SC 29808

(803) 725-1827
(803) 725-3637

Outline

- General Comments
- OpenVMS Operating Systems
- UNIX Operating Systems
- Macintosh
- IBM PCs and Clones
- Response Organizations
- General Topics
- Summary

General Comments

This will not be an Internet tutorial but rather information about tools and locations that will allow a computer security professional to search the Internet for security related information.

OpenVMS Operating Systems

- **Anonymous FTP list from csvax1.ucc.ie**
- **A good list of nodes to start with:**
  - **FileServ@wkuvx1.bitnet,**
  - **VmsServ@bay.cc.kcl.ac.uk,**
  - **http://www.wku.edu/,**
  - **ftp.spc.edu,**
  - **uduniv.cc.uniud.it,**
  - **narnia.memphis.edu,**
  - **wuarchive.wustl.edu.**

  NOTE: For specific locations, check the list on csvax1.
- **DECUS CD-ROM collections**

OpenVMS Programs

AUTOLOGOFF	**Procedure to automatically log yourself out.**
CRYPT	**Crypt/Decrypt files**
ETHERMON	**Monitor packets, MAC Addresses & protocols on ethernet line**
EYESPY	**Watch for a specific user to log on**
IDENT	**Show who holds an identifier , or what identifiers a user holds**
JOBLOG	**Log session to a file**
LAST	**Displays Last login info for accounts**
LTMONITOR	**Idle terminal killer**
MASTER	**Delegate GRANT/REVOKE of groups of identifiers**
OPCON	**Menu driven operator interface**
PGP	**Pretty Good Privacy (Encryption)**
READPROXY	**Display remote proxies to a given local username**

OpenVMS Programs (cont)

SCANUAF	**Scan SYSUAF for accounts matching specified criteria**
SUPERVISOR	**Supervisor series of utilities - Photo , Observe , Advise**
TERM_LOCK_2	**Lock terminal from unauthorized access**
UAF	**Joe Meadow's UAF selection and display utility**
VERB	**Joe Meadow's utility to show command definitions**
VERSION	**Displays version info from VMS executables**
WATCHER	**Configurable idle terminal timeout manager**
XAUTOLOCK	**Automatically lock idle DECwindows sessions**
XSCOPE	**Monitor X11 Traffic**

UNIX Operating Systems

- **SOCKS**
  - **An Internet "socket server" that provides convenient and secure network connectivity through a firewall.**
- **COPS**
  - **The Computer Oracle and Password System. Examines a system for known weaknesses and alerts the system manager. Can automatically correct some problems.**
- **TIGER**
  - **A number of monitoring scripts. Similar to COPS, but more up-to-date and user friendly.**
- **TRIPWIRE**
  - **Scans file systems and computes digital signatures for the files. The digital signatures can be used later to check files for any changes.**

UNIX Operating Systems (cont)

- **CRACK**
  - » **A popular password cracking program. User can configure Crack for the types of guesses attempted.**
- **KERBEROS**
  - » **Authentication system to use on non-secure networks. Uses a key distribution model encryption system.**
- **TCP WRAPPERS**
  - » **Has become very popular recently. Provides monitoring and control over connections to TCP ports. Can be expanded to other programs using a library provided with the distribution.**

UNIX Operating Systems (cont)

- **SATAN**
  - » **System Administrator Tool for Analyzing Networks. Scans systems on a network and documents known vulnerabilities that it finds. Includes user help that explains the problems found and possible corrections.**
  - » **Be sure and read the bulletins and warnings issued by the response organizations discussed later in this talk.**
- **Merlin**
  - » **Developed by the Department of Energy's Computer Incident Advisory Capability. Provides users with a GUI interface to manage and in some cases enhance many of the available security tools for Unix.**

UNIX Operating Systems (cont)

- **Sources For Unix Security Tools**
  - **Computer Incident Advisory Capability**
    - **www - http://ciac.llnl.gov**
    - **ftp - ciac.llnl.gov**
  - **Coast**
    - **www - http://www.cs.purdue.edu**
    - **ftp - coast.cs.purdue.edu**
  - **Computer Emergency Response Team**
    - **ftp - ftp.cert.org in /pub/tools**
  - **NECTECH**
    - **ftp - ftp.nec.com in /pub/security**

Macintosh

- **Read the Frequently Asked Questions (FAQ)**
- **Macintosh FTP sites**
  - **sumex-aim.stanford.edu**
  - **mac.archive.umich.edu**
  - **wuarchive.wustl.edu (mirror of above)**
  - **mirrors.aol.com**
- **Pretty Good Privacy (PGP)**
  - **Check the "Here's How to MacPGP!" guide on one of the above sites.**
- **Anti-Virus Programs**
  - **Disinfectant**
  - **Gatekeeper**
    - **Available at ftp sites listed above and ciac.llnl.gov**

SITES FOR DOS, WINDOWS, WINDOWS 95, AND WINDOWS NT

- **Oak Software Repository**
  - **www - http://www.acs.oakland.edu/oak.html**
  - **ftp - oak.oakland.edu**
  - **Oakland University. Serves as a mirror of the Coast to Coast Software Repository, but also offers other collections to Internet users.**

SITES FOR DOS, WINDOWS, WINDOWS 95, AND WINDOWS NT (cont.)

- **AOL Mirrors**
  - **ftp - mirrors.aol.com**
  - **American Online's FTP Mirror Site**
- **Winsite**
  - **ftp - ftp.winsite.com**
  - **www - http://www.winsite.com**
  - **Considered "The Planet's Largest Software Archive for Windows"**

DOS

- **Files from Oakland /SimTel/msdos/security**
  - **pclockv2.zip**
    - **Lockup your keyboard when you need to step away.**
  - **passwrd1.zip**
    - **Password protection.**
  - **mrsafe.zip**
    - **Provides a screen saver and system protection.**
  - **dos-log.zip**
    - **Command line logging to a file.**
  - **eeklogin.zip**
    - **Restricts access to certain commands.**
  - **protdrx.zip**
    - **Boot password protection.**
  - **copynot2.zip**
    - **Restricts the ability to copy a disk.**

DOS (cont.)

- **Files from Oakland /SimTel/msdos/virus**
  - **fp-219.zip**
    - **F-Prot antivirus, version 2.19**
  - **avp21.zip**
    - **Antiviral Toolkit Pro, version 2.1**
  - **navm.zip**
    - **Norton's free Micholangelo Edition**
  - **Vsh-226e.zip**
    - **McAfee's VShield, version 2.2.6**
- **Files from CIAC /pub/ciac/sectools/pcvirus**
  - **chk4bomb.arc**
    - **Examines files for possible Trojan activity.**
  - **Be sure and check out the informational .txt files in this directory.**

NETWARE VIRUS PROTECTION

- **Files from CIAC /pub/ciac/sectools/pcvirus**
  - **3nsh160.zip**
    - **NETShield v1.60 antivirus NLM for Netware 3.x**
  - **4nsh160.zip**
    - **NETShield v1.60 antivirus NLM for Netware 4.x**

WINDOWS 3.x

- **Lockset 3.0**
  - Allows you to set restrictions on certain user actions.
  - file lockset.zip
  - AOL Mirrors in /pub/pc/win3/desktop
- **Padlock for Windows**
  - Windows locker that will close a Windows session after a certain period of time.
  - file padlock.zip
  - AOL Mirrors in /pub/pc/win3/desktop
- **ProGuard**
  - Restricts the programs that guest users can run by requiring a password
  - file prgrd-22.zip
  - AOL Mirrors in /pub/pc/win3/desktop

WINDOWS 3.x (cont.)

- **Security Program Launcher**
  - » **Similar to Proguard but with Launcher, programs are removed from the Program Manager and accessed with the Launcher.**
  - » **file seclau.zip**
  - » **AOL Mirrors in /pub/pc/win3/util**
- **WinPass 1.1**
  - » **Very good Windows password system**
  - » **file winpas11.zip**
  - » **AOL Mirrors in /pub/pc/win3/desktop**
- **WinLock**
  - » **Provides access control for multiple user system access from within Windows.**
  - » **file wlock16u.zip**
  - » **AOL Mirrors in /pub/pc/win3/desktop**

WINDOWS 3.x (cont.)

- **Microsoft Macro Virus Detector**
  - **Macro detector for Microsoft Word version 6 or later.**
  - **File mvtool10.exe**
  - **http://www.microsoft.com/msoffice/freestuf/msword/download/mvtool**

Windows 95

- **McAfee's Virus for Windows 95**
  - **file s95i110e.zip**
  - **Oakland in SimTel/win95/virus**
- **Windows 95 Menu with Security Access Control**
  - **file winu10.zip**
  - **Oakland in SimTel/win95/sysutil**
- **Simple Locking Program**
  - **File wrklck12.zip**
  - **Oakland in SimTel/win95/security**

WINDOWS NT

- **Device Locking Service**
  - » **Allows the user to lock all drives as well as com ports on the system.**
  - » **file dlock.zip**
  - » **AOL Mirrors in /pub/pc/winnt/misc**
- **Somar DumpACL - NT**
  - » **Program to dump file system and other types of permissions, audit settings, user/group information into a readable listbox format, making it easier to spot security holes.**
  - » **file dmpacl.zip**
  - » **AOL Mirrors in /pub/pc/winnt/misc**

WINDOWS NT (cont.)

- **Windows NT Tools**
  - » **Logoff, shutdown, reboot tools.**
  - » **file nttools.zip**
  - » **AOL Mirrors in /pub/pc/winnt/misc**
- **Somar DumpEvt**
  - » **Program to dump the event log in a format suitable for importing into a database.**
  - » **file dumpevt.zip**
  - » **Oakland in SimTel/nt/admin**

SOFTWARE LICENSING

- **If the product is freeware, no licensing is required.**
- **If the product is shareware, some nominal fee to the author is usually required.**
  - » **Products are usually worth a lot more than the fee charged.**
- **Please read the license requirements in the documentation supplied with the software before using it.**

RESPONSE ORGANIZATIONS

- **CIAC**
  - **Department Of Energy's Computer Incident Advisory Capability.**
  - **Contact CIAC by e-mail at ciac@llnl.gov**
  - **By Phone at (510) 422-8193**
  - **CIAC Anonymous FTP at ciac.llnl.gov**
  - **BBS at (510) 423-4753**
  - **CIAC Web Page - http://ciac.llnl.gov**
  - **E-mail list request can be completed via the Web Page**

RESPONSE ORGANIZATIONS (cont.)

- **ASSIST**
  - **Department of Defense's Automated Systems Security Incident Support Team**
  - **Contact ASSIST by e-mail at ASSIST@assist.mil**
  - **By phone at 1-800-357-4231**
  - **BBS at (703) 607-4710**
  - **ASSIST Anonymous FTP at ftp.assist.mil (available to all registered .mil addresses)**
  - **Send ASSIST e-mail list request to assist-request@assist.mil**

RESPONSE ORGANIZATIONS (cont.)

- **CERT**
  - **The Computer Emergency Response Team**
  - **Contact CERT by e-mail at cert@cert.org**
  - **By phone at (412) 268-7090**
  - **CERT Anonymous FTP at ftp.cert.org**
  - **CERT Web Page - http://www.sei.cmu.edu/technology/cert.cc.html**
  - **Send CERT e-mail list request to cert-advisory-request@cert.org or cert-tools-request@cert.org**
  - **Be sure and read the CERT FAQ which can be found in /pub**

RESPONSE ORGANIZATIONS (cont.)

- **FIRST**
  - **The Forum of Incident Response and Security Teams.**
  - **FIRST is a coalition that brings together a variety of computer security incident response teams from government, commercial, and academic organizations**
  - **Contact FIRST by e-mail at first-sec@first.org**
  - **By Phone at (301)975-3359**
  - **FIRST Web Page - http://www.first.org**

NetNews Security Groups

- **Internet equivalent of a discussion group or a "bulletin board system" (BBS)**
- **Some security related newsgroups are:**
  - **comp.security.announce**
  - **comp.security.misc**
  - **comp.security.firewalls**
  - **alt.security**
  - **alt.security.pgp**

Archie

- **Archie servers are systems which allow users to search indexes to determine what files are available on public server on the Internet.**
- **Some of the Archie servers available:**
  - **archie.ans.net 147.225.1.10 (ANS server, NY)**
  - **archie.internic.net 198.49.45.10 (AT&T server, NY)**
  - **archie.rutgers.edu 128.6.18.15 (Rutgers University)**
  - **archie.sura.net 128.167.254.195 (SURAnet server MD)**
  - **archie.unl.edu 129.93.1.14 (U. of Nebraska)**

Gopher

- Easiest way to locate Internet resources is to use the Internet Gopher ("go fer").
- Gopher is a lookup tool that allows users to probe through the Internet by using menus.
- Gopher clients for various operating systems can be downloaded from boombox.micro.umn.edu.
- Public Gopher Servers (username gopher)
  - consultant.micro.umn.edu
  - ux1.cso.uiuc.edu

WORLD WIDE WEB (WWW)

- Based on a technology called hypertext, this is the most flexible tool for searching and retrieving information from the Internet.
- Best attempt yet to organize information on the Internet. Information is stored as a set of hypertext documents and users move from one document to another via “links” established within the documents.
- Can support text, graphics, sound, and movies.
- Most easily accessed using a GUI browser (the client side) such as Mosaic or Netscape.

WORLD WIDE WEB (cont.)

- **Good sites with search engines**
  - **http://www.search.com**
  - **http://www.lycos.com**
  - **http://www.yahoo.com**
  - **http://www.altavista.digital.com**
- **Good Sites for Information**
  - **http://www.decus.org**
  - **http://www.netscape.com**
  - **http://www.eff.org**
  - **http://www.cis.ohio-state.edu**

WORLD WIDE WEB (cont.)

- **Good Sites for Information**
  - **http://www.arlut.utexas.edu/csd/sysadmin/security.html**
  - **http://nsi.nsi.org**
  - **http://hightop.nrl.navy.mil**
  - **http://www.gocso.com**
  - **http://tezcat.com/web/security/**
  - **http://www.ccd.bnl.gov**
  - **Of course, all those operated by the Response Organizations.**

BOOKS/DOCUMENTS/PAPERS

- **"The Whole Internet User's Guide and Catalog"**
  - **author Ed Krol**
  - **O'Reilly & Associates (ISBN: 1-56592-02-2)**
- **“The Internet Starter Kit for Macintosh”**
  - **Adam C. Engst**
  - **Published by Hayden Books (ISBN 1-56830-064-6)**
- **“The Internet Passport”**
  - **Replacement document for "NorthWestNet User Services Internet Resource Guide"**
  - **Order Form available at ftphost.nwnet.net:/user-docs/passport**

BOOKS/DOCUMENTS/PAPERS (cont.)

- **RFCs (Request For Comments)**
  - **nic.merit.edu:/documents/fyi directory.**
    - **"New Internet User Questions" (RFC-1325) is document fyi_04.txt.**
    - **"Experienced Internet User Questions" (RFC-1207) is document fyi_07.txt.**
    - **“Site Security Handbook” (RFC-1244) is document fyi_08.txt**
    - **"There’s Gold in them thar Networks!" (RFC-1402) is document fyi_10.txt.**
    - **“Privacy and Accuracy Issues in Network” (RFC-1355) is document fyi_15.txt.**
    - **"Internet Users' Glossary" (RFC-1392) is document fyi_18.txt.**
    - **"What is the Internet?" (RFC-1462) is document fyi_20.txt.**

BOOKS/DOCUMENTS/PAPERS (cont.)

- **FAQs (Frequently Asked Questions)**
  - **The USENET FAQs at:**
    - **http://www.cis.ohio-state.edu/hypertext/faq/usenet/top.html**
  - **Some good ones for Security are:**
    - **Computer Security**
    - **VIRUS-L/comp.virus.Frequently Asked Questions (FAQ)**
    - **Cryptography**
    - **Dec FAQ**
    - **Firewalls FAQ**
    - **Info Vax**
    - **Internet**
    - **Internet Services**
    - **Kerberos FAQ**

BOOKS/DOCUMENTS/PAPERS (cont.)

- **FAQs (Frequently Asked Questions)**
  - **More good ones for Security:**
    - **Net Privacy**
    - **Pgp FAQ**
    - **FAQ: Computer Security Frequently Asked Questions**
    - **Unix FAQ**
    - **World Wide Web FAQ**
    - **computer-security/compromise-faq**

BOOKS/DOCUMENTS/PAPERS (cont.)

- **"The Hitchhiker's Guide to the Internet"**
  - **wuarchive.wustl.edu:/doc/EFF/Net_info/Guidebooks directory as hitchhikers.guide.gz**
- **"The Internet Companion"**
  - **ftp.std.com:/OBS/The.Internet.Companion directory.**
  - **This is part one of the Tracy LaQuey's book of the same name.**
- **"Zen and the Art of Internet"**
  - **ftp.std.com:/obi/Internet/zen-1.0 directory as zen-1.0.txt.Z**

BOOKS/DOCUMENTS/PAPER (cont.)

- **Bruce Sterling's "The Hacker Crackdown"**
  - **ftp.eff.org:/pub/Publications/Bruce_Sterlings/Hacker**
- **"EFF's (Extend) Guide to the Internet"**
  - **"A round trip through Global Networks, Life in Cyberspace, and Everything..."**
  - **ftp.eff.org:/pub/Net_info/EFF_Net_Guide**
  - **Replaces the "Big Dummy's Guide to the Internet"**

Summary

There's a lot of good information/tools out there if:

- **You know where to look or know how to find a source,**
- **You're very selective in what you download...don't try to get it all,**
- **You're careful...always test in a stand-alone environment,**
- **You stay informed...browse through the security newsgroups or get yourself on a distribution list or two...just don't try them all.**

QUESTIONS?

ANSWERS?

SUGGESTIONS?